儿童手表安全性研究

中北大学-刘波

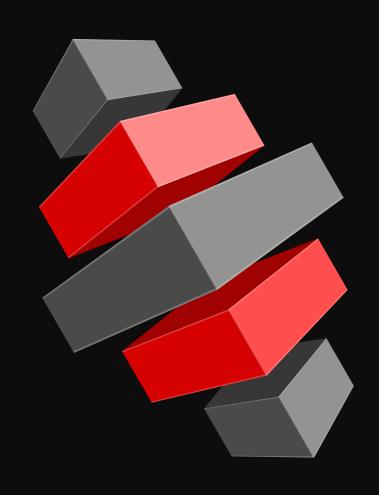


目录

- 1 绑定连接过程
- 2 手表安全措施
- 3 可能的攻击面
- 4 两种攻击场景



绑定连接过程



- 将SIM卡放到手表内,开机,显示激活二维码
- 手机下载360儿童卫士,登录360账号
- 扫描二维码,输入手表SIM卡号
- 验证二维码,验证手机号
- 绑定成功



手表安全措施



一键SOS

远程拍照

安全区域

运动轨迹

蓝牙防走散

数据安全

自动拦截陌生来电

位置信息双重加密

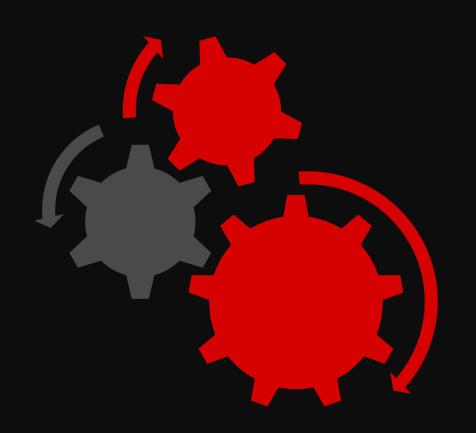
单向语音监听 昭名端现点监禁

服务端双向鉴权





手表安全措施





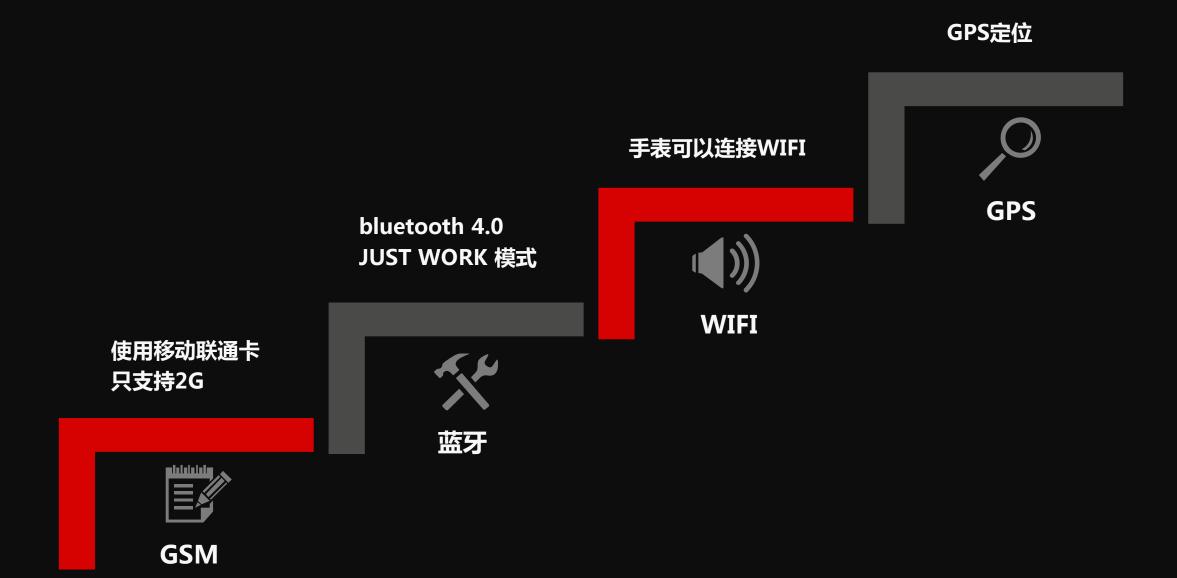
通体只有一个按钮,激活后,不能主动关机,避免 儿童误挤压关闭儿童手表导致的安全措施失效。



一直开启GPRS数据,时刻同服务端进行数据交换



可能的攻击面



可能的攻击面

单击此处添加您的内容。



单击此处添加您的内容。



单击此处添加您的内容。



单击此处添加您的内容。





单击此处添加您的内容。



单击此处添加您的内容。

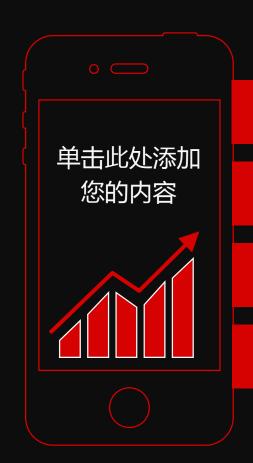


单击此处添加您的内容。



单击此处添加您的内容。

可能的攻击面



单击此处添加您的内容。

1

单击此处添加您的内容。

2



单击此处添加您的内容。

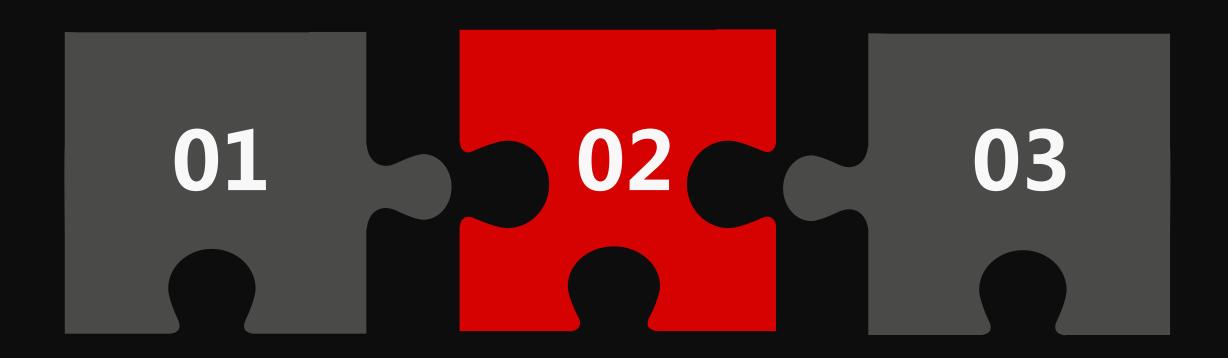
单击此处添加您的内容。建议您在展示时采用微软雅黑字体。

3

单击此处添加您的内容。建议您在展示时采用微软雅黑字体。

4





家长带领儿童去 客流量多的景区 或者顾客多的大型商场 架设无线电发射台,攻击 SOS、蓝牙防走散、语音监 听、远程拍照、定位等功能 实施攻击 拐走儿童

蓝牙防走散 手机蓝牙 蓝牙4.0在低功耗状态下工作时,几乎不耗电、请放 心使用。 宝贝 蓝牙防走散 已进入蓝牙防走散 手表蓝牙状态 "蓝牙防走散"功能需要将手表蓝牙打开 开启后,宝贝在身边时将自动进入蓝牙防走散,需要手 (1) 机和手表都打开蓝牙,手表离手机超出一定距离就会报 警。建议外出旅行逛街时开启。

```
<string name="add_watch_error_49">手表正处于蓝牙防走散不能响应请求</string>
<string name="ble close hint">已关闭,手表蓝牙可到"我的-更多设置"中关闭。其他手表不变</string>
<string name="ble open hint">已开启,手表蓝牙也会被同步开启</string>
<string name="ble tips contents">蓝牙防走散在陌生区域中断会用红色警报提醒家长。在安全区域内断开则以较弱的橙色警报替代。为避免打扰,也可以关闭在安全区域
<string name="bt close monitor">已关闭蓝牙防走散</string>
<string name="bt_connect_monitor_success">已进入蓝牙防走散</string>
<string name="bt_connect_promot">当%1$s在您的身边时,手表将自动进入蓝牙防走散。</string>
<string name="bt_connected_status_text">蓝牙防走散</string>
<string name="bt desc">蓝牙 4.0在低功耗状态下工作时,几乎不耗电,请放心使用。</string>
<string name="bt dont support">您的手机不支持此功能(需手机支持蓝牙4.0且安卓版本在4.3及以上)</string>
<string name="bt_in_monitor">%1$s在当前位置处于蓝牙防走散</string>
<string name="bt_monitor_connected_with_me">我和%1$s处于蓝牙防走散</string>
<string name="bt_monitor_connected_with_other">%1$s和%2$s处于蓝牙防走散</string>
<string name="bt monitor opend bt dialog content">蓝牙防走散下,将会开启并使用手机的蓝牙功能。</string>
<string name="bt monitor opend bt dialog content">蓝牙防走散下,将会开启并使用手机的蓝牙功能。</string>
<string name="bt_monitor_opend_bt_dialog_title">开启蓝牙 </string>
<string name="bt_monitor_opend_net_dialog_content"><mark>蓝牙</mark>防走散下手表会依赖手机客户端定位并进入低功耗模式,为了能够正常定位,请确认手机处于联网状态。<
<string name="bt monitor radio title">蓝牙防走散</string>
<string name="bt_not_open">请先打开列表顶端的蓝牙开关</string>
<string name="bt setting close">手机蓝牙:已关闭</string>
<string name="bt_setting_close_bt">将关闭手机的蓝牙。</string>
<string name="bt setting dlg title close bt">关闭蓝牙 </string>
<string name="bt_setting_dlg_title_open_bt">开启蓝牙 </string>
<string name="bt_setting_open">手机蓝牙:已开启</string>
<string name="bt_setting_open_bt">将开启手机的蓝牙。</string>
<string name="bt setting tips">开启后,宝贝在身边时将自动进入蓝牙防走散需要手机和手表都打开蓝牙,手表离手机超出一定距离就会报警。建议外出旅行逛街时开启
<string name="bt setting tips">开启后,宝贝在身边时将自动进入蓝牙防走散需要手机和手表都打开蓝牙,手表离手机超出一定距离就会报警。建议外出旅行逛街时开启
<string name="connected monitor">%1$s已进入蓝牙防走散</string>
<string name="disconnected_monitor">%1$s已退出蓝牙防走散</string>
<string name="permission_location_bt_fail">获取定位权限失败, 蓝牙 防走散功能需要定位权限,请开启该权限</string>
<string name="setting_blue">蓝牙防走散</string>
<string name="settings is bt dont disturb sub">安全区内断开蓝牙防走散时响橙色警报,关闭则不提醒</string>
<string name="settings is monitor">蓝牙防走散</string>
<string name="watch_setting_blue_close">已关闭,手表蓝牙需您手动关闭</string>
<string name="watch_setting_blue_open">已开启,手表蓝牙也会被同步开启</string>
<string name="watch_setting_blue_status">手表蓝牙状态</string>
<string name="watch setting blue status hint"> "蓝牙 防走散" 功能须要手表蓝牙打开</string>
<string name="watch setting blue status hint"> "蓝牙防走散" 功能须要手表蓝牙打开</string>
```



★ Bluetooth LE scanner



360KidsWatch : CF:53:5E:76:0A:39 rssi=-64 time=757 Scanner stop

P.nbr.	Time (us) +0 =0	Channel 0x25	Access Address 0x8E89BED6	Adv PDU Type ADV_IND	Type 0		PDU Head RxAdd 0	der PDU-Length 24	AdvA 0xCF535E760A39	03 03 30 76 0A 39	AdvData E0 07 FF CF 53 5E 05 12 D0 07 20 03	CRC 0x838BB3	RSSI (dBm) -56	FCS OK		^
P.nbr. 2	Time (us) +246252 =246252	Channel 0x25	Access Address 0x8E89BED6	Adv PDU Type ADV_IND	Type 0		PDU Head RxAdd 0	der PDU-Length 24	AdvA 0xCF535E760A39	03 03 30 76 0A 39	AdvData E0 07 FF CF 53 5E 05 12 D0 07 20 03	CRC 0x838BB3	RSSI (dBm) -57	FCS OK		
P.nbr.	Time (us) +243751 =490003	Channel 0x25	Access Address 0x8E89BED6	Adv PDU Type ADV_IND	Type 0		PDU Head RxAdd 0	der PDU-Length 24	AdvA 0xCF535E760A39	03 03 30 76 0A 39	AdvData E0 07 FF CF 53 5E 05 12 D0 07 20 03	CRC 0x838BB3	RSSI (dBm) -53	FCS OK		
P.nbr. 4	Time (us) +246252 =736255	Channel 0x25	Access Address 0x8E89BED6	Adv PDU Type ADV_IND	Type 0		PDU Head RxAdd 0	der PDU-Length 24	AdvA 0xCF535E760A39	03 03 30 76 0A 39	AdvData E0 07 FF CF 53 5E 05 12 D0 07 20 03	CRC 0x838BB3	RSSI (dBm) -46	FCS OK		
P.nbr.	Time (us) +241251 =977506	Channel 0x25	Access Address 0x8E89BED6	Adv PDU Type ADV_IND	Type 0		PDU Head RxAdd	PDU-Length	AdvA 0xCF535E760A39	03 03 30 76 0A 39	AdvData E0 07 FF CF 53 5E 05 12 D0 07 20 03	CRC 0x838BB3	RSSI (dBm) -46	FCS OK		
P.nbr.	Time (us) +242502 =1220008	Channel 0x25	Access Address 0x8E89BED6	Adv PDU Type ADV_IND	Type 0	Adv TxAdd	PDU Hea	der PDU-Length 24	AdvA 0xCF535E760A39	03 03 30 76 0A 39	AdvData E0 07 FF CF 53 5E 05 12 D0 07 20 03	CRC 0x838BB3	RSSI (dBm)	FCS		
P.nbr.	Time (us) +242502 =1462510	Channel 0x25	Access Address 0x8E89BED6	Adv PDU Type ADV IND	Type 0		PDU Hea		AdvA 0xCF535E760A39	03 03 30 76 0A 39	AdvData E0 07 FF CF 53 5E 05 12 D0 07 20 03	CRC 0x838BB3	RSSI (dBm)	FCS		~
7															2	>
<																

P.nbr.	Time (us) +246251	Channel	Access Address	Adv PDU Ty	pe Type	Adv PDU H TxAdd RxAd		AdvA	Ad 03 03 30 E0	vData 07 FF (CF 53 5E	CRC	RSSI (dBm)	FCS			^
16	=3666273	0x25	0x8E89BED6	ADV_INI	0	1 0	24	0xCF535E760A39	76 0A 39 05	12 D0 (07 20 03	0x838BB3	-57	OK			
P.nbr.	+423		Access Address	Adv PDU T	Type		Header Add PDU-Length		AdvA		CRC	RSSI (dBm) FCS					
17	=3666696	0x25	0x8E89BED6	ADV_SCAN	REQ 3	1	1 12	0x6520CD029964	0xCF535E760	0A39	0x2524C4	-30 OK					
P.nbr.	Time (us) +326		Access Address	Adv PDU T	ype Type	Adv PDU TxAdd Rx	Header Add PDU-Length	AdvA	ScanRspData None	CR	(dB						
18	=3667022	0x25	0x8E89BED6	ADV_SCAN	RSP 4	1	0 6	0xCF535E760A39		0x8E	0C4E -5	7 OK					
P.nbr.	Time (us) +240926	Channel	Access Address	Adv PDU	Type T	Adv ype TxAdd	PDU Header RxAdd PDU-Len	gth InitA	Adv	νA	AccessA	ddr CRCI		Data (Pari WinSize		Interval	Later
19	=3907948	0x25	0x8E89BED6	ADV_CONN	CT_REQ	5 1	1 34	0x6520CD029	964 0xCF535E	E760A39	0x15984	3EF 1A E	7 FF	08	0x0006	0x0020	0x000
P.nbr.	Time (us) +10063 =3918011	Channel 0x0E	Access Address 0x159843EF	Direction M->S	ACK Status	Data Type Control	Data H	MD PDU-Length	LL_Opcoo		FeatureS	Feature_Req		CRC 0x68EC	RSSI (dBm) -39 OK		
20	=	ONOL	UNISSUASEE	11-75	OR	CONCLOT		0 9	reacure_keq		00 00 00	00 00 00	OU EI	ONCOLC	,95 -59 OK		
P.nbr.	Time (us) +303	Channel	Access Address	Direction	ACK Status	Data Type	LLID NESN SN	Header I MD PDU-Lengtl	CRC	RSSI (dBm)	FCS						
21	=3918314	0x0E	0x159843EF	S->M	OK	Empty PDU	1 1 0	0 0	0x5F3253	-34	OK						
P.nbr.	Time (us) +39697	Channel	Access Address	Direction	ACK Status	Data Type	Data	Header MD PDU-Lengtl	CRC	RSSI (dBm)	FCS						
22 <	=3958011	0x1C	0x159843EF	M->S	OK	Empty PDU	1 1 1	0 0	0x5F3FF5	-31	OK						>

P.nbr.	Time (us) +39769	Channel	Access Address	Direction	ACK Status	Data Type	LLID NESN	Data H	eade MD	r PDU-Length	CRC	RSSI (dBm)	FCS	^
186	=4763013	0x1E	0x159843EF	M->S	OK	Empty PDU	1 0	0	0	0	0x5F3480	-32	OK	
P.nbr.	Time (us) +231	Channel	Access Address	Direction	ACK Status	Data Type	LLID NESN	Data H		r PDU-Length	CRC	RSSI (dBm)	FCS	
	=4763244	0x1E	0x159843EF	S->M	OK	Empty PDU	1 1	0	0	0	0x5F3253	-39	OK	
P.nbr.	Time (us) +39769	Channel	Access Address	Direction	ACK Status	Data Type	LLID NESN	Data H	leade MD	r PDU-Length	CRC	RSSI (dBm)	FCS	
188	=4803013	0x07	0x159843EF	M->S	OK	Empty PDU	1 1	1	0	0	0x5F3FF5	-40	OK	
P.nbr.	Time (us) +231	Channel	Access Address	Direction	ACK Status	Data Type	LLID NESN	Data H	leade MD	r PDU-Length	CRC	RSSI (dBm)	FCS	
189	=4803244	0x07	0x159843EF	S->M	OK	Empty PDU	1 0	1	0	0	0x5F3926	-36	OK	
P.nbr.	Time (us) +39770	Channel	Access Address	Direction	ACK Status	Data Type	LLID NESN	Data H	leade MD	r PDU-Length	CRC	RSSI (dBm)	FCS	
190	=4843014	0x15	0x159843EF	M->S	OK	Empty PDU	1 0	0	0	0	0x5F3480	-31	OK	
P.nbr.	Time (us) +230	Channel	Access Address	Direction	ACK Status	Data Type	LLID NESN	Data H		r PDU-Length	CRC	RSSI (dBm)	FCS	
191	=4843244	0x15	0x159843EF	S->M	OK	Empty PDU	1 1	0	0	0	0x5F3253	-42	OK	
	Time (us) +39770		Access Address 0x159843EF	Direction M->S	ACK Status	Data Type	LLID NESN	Data H	MD	r PDU-Length	CRC	RSSI (dBm)	FCS OK	V
192 <	=4883014	0x23	UX159843EF	n->5 I	ı ok i	EMBCV PD01	1	1	U	0	0x5F3FF5	-36	II OK I	>

P.nbr.	Time (us) +39771	Channel	Access Address	Direction	ACK Status	Data Type	LLID N		ata Head SN MD		ngth	CRC	RSSI (dBm)	FCS
939	=20603084	0x18	0x159843EF	M->S	OK	Empty PDU	1	0	0 0	0		0x5F3480	-30	OK
P.nbr.	Time (us) +231	Channel	Access Address	Direction	ACK Status	Data Type	LLID N		ata Head SN MD		ngth	CRC	RSSI (dBm)	FCE
940	=20603315	0x18	0x159843EF	S->M	OK	Empty PDU	1	1	0 0	0		0x5B3253	-78	ERRO
P.nbr.	Time (us) +39770	Channel	Access Address	Direction	ACK Status	Data Type	LLID N		ata Head SN MD		ngth	CRC	RSSI (dBm)	FCS
941	=20643085	0x01	0x159843EF	M->S	OK	Empty PDU	1	1	1 0	0		0x5F3FF5	-35	OK
P.nbr.	Time (us) +40000	Channel	Access Address	Direction	ACK Status	Data Type	LLID N		ata Head SN MD		ngth	CRC	RSSI (dBm)	FCS
942	=20683085	0x0F	0x159843EF	M->S	RETRY	Empty PDU	1	1	1 0	0		0x5F3FF5	-36	OK
P.nbr.	+40001			Direction	ACK Status	Data Type	LLID N	NESN		D PDU-Le	ngth		RSSI (dBm)	II——I
943	=20723086	0x1D	0x159843EF	M->S	RETRY	Empty PDU	1	1	1 0	0		0x5F3FF5		$\overline{}$
P.nbr.	Time (us) +40002	Channel	Access Address	Direction	ACK Status	Data Type	LLID N		ata Head SN MD		ngth	CRC	RSSI (dBm)	FCS
944	=20763088	0x06	0x159843EF	M->S	RETRY	Empty PDU	1	1	1 0	0		0x5F3FF5	-52	OK
P.nbr.	+40000		Access Address				LLID N	D: NESN	ata Head SN MD	<mark>der</mark> D PDU-Le	ngth		RSSI (dBm)	
945	=20803088	0x14	0x159843EF	M->S	RETRY	Emptv PDU	1	1	1 0	0		0x5F3FF5	-48	OK I

P.nbr.	Time (us) +40001	Channel	Access Address	Direction	ACK Status	Data Type	LLID	NESN	Data H	eade MD	PDU-Length	CRC	RSSI (dBm)	FCS
1032	=24083160	0x15	0x159843EF	M->S	RETRY	Empty PDU	1	0	0	0	0	0x5F3480	-34	OK
P.nbr.	Time (us) +40001	Channel	Access Address	Direction	ACK Status	Data Type	LLID	NESN	Data H	eade MD	r PDU-Length	CRC	RSSI (dBm)	
1033	=24123161	0x23	0x159843EF	M->S	RETRY	Empty PDU	1	0	0	0	0	0x5F3480	-33	OK
	+40001		Access Address			Data Type	LLID	NESN		MD	PDU-Length	CRC	RSSI (dBm)	
	=24163162	0x0C	0x159843EF	M->S	RETRY	Empty PDU	1	0	0	0	0	0x5F3480	-34	OK
P.nbr.	Time (us) +40001	Channel	Access Address	Direction	ACK Status	Data Type	LLID	NESN	Data H	eade MD	r PDU-Length	CRC	RSSI (dBm)	
	=24203163	0x1A	0x159843EF	M->S	RETRY	Empty PDU	1	0	0	0	0	0x5F3480	-30	OK
	+40000	Channel	Access Address	Direction	ACK Status	Data Type	LLID	NESN	Data H SN	eade MD	r PDU-Length	CRC	RSSI (dBm)	
1036	=24243163	0x03	0x159843EF	M->S	RETRY	Empty PDU	1	0	0	0	0	0x5F3480	-36	OK
P.nbr.	+40002		Access Address			Data Type	LLID	NESN	Data H SN		r PDU-Length		RSSI (dBm)	
1037	=24283165	0x11	0x159843EF	M->S	RETRY	Empty PDU	1	0	0	0	0	0x5F3480	-34	OK
	Time (us) +40000 =24323165		Access Address 0x159843EF	Direction M->S		Data Type Empty PDU	LLID	NESN	Data H	eade MD	PDU-Length	CRC 0x5F3480	RSSI (dBm) -31	
<	-243231631	OXIL	0213504351	M-25	REIRI	EMDCV PD0		·			0	0x3F3400	-31	II OK I



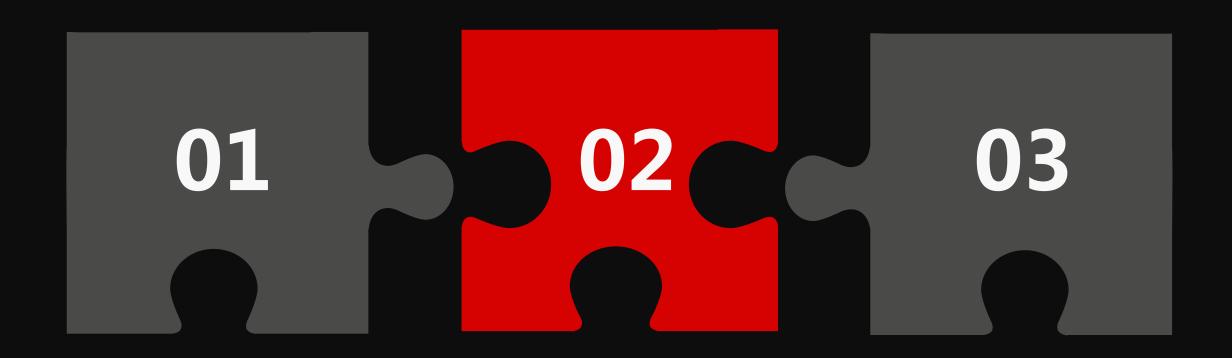
OpenBTS

通过把手表的通信全部定向到伪基站,来攻击手表的SOS、蓝牙防走散、语音监听、远程拍照、定位等功能



GPS-SIM

通过欺骗手表的GPS,攻击手表的安全区域等功能。



儿童带着手表在幼儿园的活 动场所玩耍 连接手表蓝牙,获取手表内 信息,如家长电话号码 实施社会工程学攻击 进行诈骗和勒索

P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type		Adv	PDU Head	der	AdvA		AdvData	CRC	RSSI	FCS	
rbr.	+0	Chamilei	Access Address	Aut 1 bo Type	Type	TxAdd	RxAdd	PDU-Length	AUVA	03 03 3	30 E0 07 FF CF 53 5E	CAC	(dBm)	103	
1	=0	0x25	0x8E89BED6	ADV_IND	0	1	0	24	0xCF535E760A39	76 OA 3	39 05 12 D0 07 20 03	0x838BB3	-56	OK	
	Time (us)					Adv	PDU Head	der			AdvData		RSSI		
P.nbr.	Time (us) +246252	Channel	Access Address	Adv PDU Type	Type			PDU-Length	AdvA	03 03 3	30 E0 07 FF CF 53 5E	CRC	(dBm)	FCS	
2	=246252	0x25	0x8E89BED6	ADV IND	0	1	0	24	0xCF535E760A39	76 OA 3	39 05 12 D0 07 20 03	0x838BB3	-57	OK	
P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type			PDU Head		AdvA		AdvData	CRC	RSSI	FCS	
	+243751				Type	TxAdd	RxAdd	PDU-Length			30 E0 07 FF CF 53 5E		(aBm)		
3	=490003	0x25	0x8E89BED6	ADV_IND	0	1	0	24	0xCF535E760A39	76 0A 3	39 05 12 D0 07 20 03	0x838BB3	-53	OK	
D L	Time (us)	011		A di PRUT		Adv	PDU Head	der			AdvData	one	RSSI		
P.nbr.	+246252	Channel	Access Address	Adv PDU Type	Type	TxAdd	RxAdd	PDU-Length	AdvA	03 03 3	80 E0 07 FF CF 53 5E	CRC	(dBm)	FCS	
4	=736255	0x25	0x8E89BED6	ADV_IND	0	1	0	24	0xCF535E760A39	76 OA 3	39 05 12 D0 07 20 03	0x838BB3	-46	OK	
	Time (ue)					Adv	PDU Head	dor			AdvData		Deel	$\overline{}$	
P.nbr.	Time (us) +241251	Channel	Access Address	Adv PDU Type	Type	TxAdd	RxAdd	PDU-Length	AdvA	03 03 3	AdvData 30 E0 07 FF CF 53 5E	CRC	RSSI (dBm)	FCS	
	=977506	0x25	0x8E89BED6	ADV IND	0	1	0	24	0xCF535E760A39	76 03 3	89 05 12 DO 07 20 03	0x838BB3	-46	OK	
	-577500	UNLU	ONOLOJBEDO	ADV_IND	_			24	OACE SSSETOGROS	70 OR 3	77 03 12 20 07 20 03	OXOSOBBS			
P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type		Adv	PDU Hea		AdvA		AdvData	CRC	RSSI		
	+242502				Type	TxAdd	RxAdd	PDU-Length		03 03	30 E0 07 FF CF 53 5E		(dBm)	.	
6	=1220008	0x25	0x8E89BED6	ADV_IND	0	1	0	24	0xCF535E760A39	76 0A	39 05 12 D0 07 20 03	0x838BB3	-55	OK	
	Time (us)					Adv	PDU Hea	der			AdvData		RSSI		
P.nbr.	Time (us) +242502	Channel	Access Address	Adv PDU Type	Type	TxAdd	RxAdd	PDU-Length	AdvA	03 03	30 E0 07 FF CF 53 5E	CRC	(dBm)	FCS	
7	=1462510		0x8E89BED6	ADV IND	0	1	0	24	0xCF535E760A39	76 OA	39 05 12 D0 07 20 03	0x838BB3		OK	
<															>

蓝牙4.0的几种配对方式

Numeric Comparison:配对双方都显示一个6位的数字,由用户来核对数字是否一致,一致即可配对。例如手机之间的配对。

Just Works:用于配对没有显示没有输入的设备,主动发起连接即可配对,用户看不到配对过程。例如连接蓝牙耳机。

Passkey Entry:要求配对目标输入一个在本地设备上显示的6位数字,输入正确即可配对。例如连接蓝牙键盘。

Out of Band:两设备的通过别的途径交换配对信息,例如NFC等。例如一些NFC蓝牙音箱。

Classic中这四个配对方式就是SSP简单配对中四种模式。蓝牙配对流程主要防止两种攻击,MITM中间人攻击以及passive eavesdropping被动监听攻击。这四种配对方式,除开JUSTWORK外,都可以防止这两种攻击。JUSTWORK由于不涉及人机交互,所以没法防止MITM的中间人攻击。(插一句,传统蓝牙的PIN CODE配对方式就是由于无法防止被动监听攻击(穷举PIN码)才衍生了这四种SSP简单配对方式。)

2. BLE中LE配对分为4.0版本中的LE LEGACY配对方式以及在BLE4.2版本开始导入的BLE Secure Connection配对方式。

前者LEGACY中,配对方式三种,JUSTWORK,PASSKEY ENTRY,以及OOB,JUSTWORK 依然无法防止MITM,另外由于秘钥生成方式的缺陷,导致LE LEGACY配对方式无法防止被动 监听攻击(OOB可以防止,因为用了非空中的传输交互)

正因为此,BLE4.2版本把Secure connection也引入到了BLE中(为什么说也,是因为CLASSIC模式中也有SECURE CONNECTION方式…),

BLE Secure connection和CLASSIC 的SSP采用同样的ECDH加密方式,所以安全性恢复到同样等级,可以防止被动监听攻击了。BLE SECURE CONNECTION配对又有了四种配对模式,JUSTWORK, PASSKEY ENTRY, NUMERIC COMP.,以及OOB,同样类同于SSP,JUSTWORK防止不了MITM。

谢谢

THANK YOU FOR YOUR LISTENING

中北大学-刘波

